Protected B

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2020-04-17 THRU 2020-10-17

VERSION: 1.2
DATE: 2020-04-16

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-07	COVID 19 – Contact tracking Mobile Application Beta – *Valid 2020-04-07 thru 2020-04-17*	
1.2	2020-04-16	CANArrive Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Business owner: John Ommanney, Director General, Travellers Programs	
Conditions:	**Digital Signature /Date**
Service Owner: Cameron MacDonald, Director General, Business Application Services	
Conditions:	**Digital Signature /Date** Cameron MacDonald 2020-04-16
CBSA Chief Technology Officer: Daniel Tremblay, CTO and Director General, Enterprise Services	
Conditions:	**Digital Signature /Date**
Chief Security Officer: Pierre Lessard, Chief Security Officer (CSO)	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Signature numérique de LESSARD PIERRE Date : 2020.04.16 16:31:28 -04'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Summary of Authorization Package

2.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
Covid-19 Contact Tracking Desktop Application	2020-04-03	N		N/A
Covid-19 Contact Tracking Mobile App	2020-04-15	N		N/A

2.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

2.2.1 Covid-19 Contact Tracking Desktop Application – 2020-04-03

This application has a level of assessed risk, for which the target level of acceptable residual risk is Low. This Interim Security Authorization provides an interim authority to Operate with an expiry date of October 3rd, 2020, to process information up to and including Protected B service delivery information with availability commencing immediately following approval of this document with the following conditions:

1.

2.

3.

2.2.2 CANArrive Mobile Application Release 1 – 2020-04-16

This application has a level of assessed risk, for which the target level of acceptable residual risk This Interim Security Authorization provides an interim authority to operate for release 1 with an expiry date of October 17th 2020 (6 months), to process information up to and including Protected B service delivery information with availability commencing immediately following approval of this document with the following conditions:

1.

2.

Protected B

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2021-07-05 THRU 2022-07-05

VERSION: 1.3
DATE: 2021-06-30

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Service Owner: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** UTANO ANTONIO Digitally signed by UTANO ANTONIO Date: 2021.07.04 12:32:42 -04'00'
CBSA Chief Technology Officer: Daniel Tremblay, CTO and Director General, IT Solutions and Operations	
Conditions:	**Digital Signature /Date** FORBERG ANDREW Digitally signed by FORBERG ANDREW Date: 2021.07.02 16:16:44 -04'00'
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2021.06.30 16:45:46 -04'00'
Chief Security Officer: Pierre Lessard, CSO and Director General Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Signature numérique de LESSARD PIERRE Date : 2021.07.02 17:04:13 -04'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Summary of Authorization Package

2.1 ArriveCan v2.19 – Proof of Vaccine (PVC)

This application has a level of assessed risk, for which the target level of acceptable residual risk This Interim Security Authorization provides an interim authority to Operate with an expiry date of July 4th, 2022, to process information up to and including Protected B service delivery information with availability commencing immediately following approval of this document with the following conditions:

1. The Security Management Action Plan (SMAP) form is completed and the form is signed off within 30 business days of go live.
2. The commitments made through the SMAP process are met based on timelines specified in the SMAP.

2.2 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracking Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-06-30	Y		improved

2.3 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**Border Operations Service-BOS**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	Final Security Assessment Report (FSAR), Security Management Action Plan (SMAP)	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2021-10-18 THRU 2022-10-18

VERSION: 1.4
DATE: 2021-10-18

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO *Valid 2021-10-18 thru 2022-10-18*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

<table>
<tr><td colspan="2">I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2.
I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context.
The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.</td></tr>
<tr><td colspan="2"><b>Service Owner</b>: Antonio Utano, a/Director General, Border Technologies Innovation</td></tr>
<tr><td><b>Conditions:</b></td><td><b>Digital Signature /Date</b>
UTANO ANTONIO
Digitally signed by UTANO ANTONIO
Date: 2021.11.03 12:53:49 -04'00'</td></tr>
<tr><td colspan="2"><b>CBSA Chief Technology Officer:</b> Daniel Tremblay, CTO and Director General, IT Solutions and Operations</td></tr>
<tr><td><b>Conditions:</b>
This ISA represents a platform that has not yet operationally transitioned to ITSO; when it does, a re-evaluation of its risk posture will be required.</td><td><b>Digital Signature /Date</b>
TREMBLAY DANIEL
Digitally signed by TREMBLAY DANIEL
DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057
Reason: I am the author of this document
Location: your signing location here
Date: 2021-10-25 20:42:50
Foxit PhantomPDF Version: 10.0.1</td></tr>
<tr><td colspan="2"><b>Cyber Security:</b> Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services</td></tr>
<tr><td><b>Conditions:</b></td><td><b>Digital Signature /Date</b>
LECHASSEUR GINO
Signature numérique de LECHASSEUR GINO
Date : 2021.10.22 12:20:09 -04'00'</td></tr>
<tr><td colspan="2"><b>Chief Security Officer:</b> Pierre Lessard, CSO and Director General, Security and Professional Standards</td></tr>
<tr><td><b>Conditions:</b></td><td><b>Digital Signature /Date</b>
LESSARD PIERRE
Digitally signed by LESSARD PIERRE
Date: 2021.10.25 07:29:21 -04'00'</td></tr>
</table>

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Summary of Authorization Package

2.1 ArriveCan v2.22 – BSO

This application has a [redacted] level of assessed risk, for which the target level of acceptable residual risk [redacted] This Interim Security Authorization provides an interim authority to Operate with an expiry date of Oct 18th, 2022, to process information up to and including Protected B service delivery information with [redacted] availability commencing immediately following approval of this document with the following conditions:

1. The Security Management Action Plan (SMAP) form is completed and the form is signed off within 30 business days of go live.
2. The commitments made through the SMAP process are met based on timelines specified in the SMAP.

2.2 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracking Desktop Application	2020-04-03	N	[redacted]	N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-06-30	Y		improved

2.3 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**Border Operations Service-BOS**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	Final Security Assessment Report (FSAR), Security Management Action Plan (SMAP)	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VERSION: 1.5
DATE: 2021-10-26

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO *Valid 2021-10-18 thru 2022-10-18*	
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

SIGNATURE PAGE

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: Calvin Christiansen, Director General, COVID - 19 Border Task Force	
Conditions:	**Digital Signature /Date** CHRISTIANSEN CALVIN Digitally signed by CHRISTIANSEN CALVIN Date: 2021.11.08 08:29:36 -05'00'
Service Owner: Carol Sabourin, Executive Director, Project and Service Management Oversight	
Conditions:	**Digital Signature /Date** SABOURIN CAROL Digitally signed by SABOURIN CAROL Date: 2021.11.08 09:42:34 -05'00'
CBSA Chief Technology Officer: Dave Beach, Executive Director, IT Operations	
Conditions:	**Digital Signature /Date** BEACH DAVE Digitally signed by BEACH DAVE Date: 2021.11.03 19:41:21 -04'00'
Cyber Security: Steven Proulx, Director, Cyber Security and IT Continuity	
Conditions:	**Digital Signature /Date** PROULX STEVEN Digitally signed by PROULX STEVEN Date: 2021.10.27 10:37:33 -04'00'
Chief Security Officer: Matthew Kletke, Director, Infrastructure and Information Security	
Conditions:	**Digital Signature /Date** KLETKE MATTHEW Digitally signed by KLETKE MATTHEW Date: 2021.10.28 08:04:26 -04'00'

Section 1 | SECURITY AUTHORIZATION (SA) CONTENT

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Summary of Authorization Package

2.1 R1867 – Mandatory Random Testing

This application has a [redacted] level of assessed risk, for which the target level of acceptable residual risk [redacted] This Security Authorization provides an Authority to Operate (ATO), to process information up to and including Unclassified service delivery information with [redacted] availability commencing immediately following approval of this document.

2.2 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracking Desktop Application	2020-04-03	N	[redacted]	N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-06-30	Y		Improved
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A

2.3 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracking applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
R1867 MRT	MRT	Final Security Assessment Report (FSAR),	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	FSAR, Security Management Action Plan (SMAP)	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2021-11-26 THRU 2022-11-26

VERSION: 1.6
DATE: 2021-11-25

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO *Valid 2021-10-18 thru 2022-10-18*	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: Calvin Christiansen, Director General, COVID-19 Border Task Force	
Conditions:	**Digital Signature /Date** Sharon Spicer Digitally signed by Sharon Spicer DN: CN=Sharon Spicer, E=sharon.spicer@cbsa-asfc.gc.ca Reason: I am approving this document Location: your signing location here Date: 2021-12-16 22:01:25 Foxit PhantomPDF Version: 10.0.1
Service Owner: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** LAUZON STEVE Digitally signed by LAUZON STEVE Date: 2021.11.25 18:51:46 -05'00'
CBSA Chief Technology Officer: Daniel Tremblay, Director General, IT Solutions and Operations	
I understand and acknowledge that the Agency has determined the business benefit represented by this service significant enough to warrant the issuance of a time-limited SA pending the more comprehensive implementation of mitigations and safeguards, and I will collaborate with other stakeholders within the Agency's prioritization framework to accomplish that.	**Digital Signature /Date** TREMBLAY DANIEL Digitally signed by TREMBLAY DANIEL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057 Reason: I am the author of this document Location: your signing location here Date: 2021-12-03 06:56:45 Foxit PhantomPDF Version: 10.0.1
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2021.11.25 16:57:49 -05'00'
Chief Security Officer: Pierre Lessard, CSO and Director General, Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Digitally signed by LESSARD PIERRE Date: 2021.11.26 09:18:53 -05'00'

Section 1 | SECURITY AUTHORIZATION (SA) CONTENT

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 BSO Mobile Lite

This application has a level of assessed risk, for which the target level of acceptable residual risk

This Interim Security Authorization provides an interim authority to Operate with an expiry date of November 26, 2022, to process information up to and including Unclassified service delivery information with availability commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracking Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-06-30	Y		Improved
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracking applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
BSO Mobile App Lite	BSO Mobile	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2021-11-29 THRU 2022-05-29

VERSION: 1.7
DATE: 2021-11-29

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO *Valid 2021-10-18 thru 2022-10-18*	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	
1.4	2021-11-29	ArriveCan v2.23 – SAVE *Valid 2021-11-29 thru 2022-05-29*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Service Owner: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** UTANO ANTONIO Digitally signed by UTANO ANTONIO Date: 2021.11.29 12:12:09 -05'00'
CBSA Chief Technology Officer: Daniel Tremblay, Director General, IT Solutions and Operations	
I understand and acknowledge that the Agency has determined the business benefit represented by this service significant enough to warrant the issuance of a time-limited SA pending the more comprehensive implementation of mitigations and safeguards, and I will collaborate with other stakeholders within the Agency's prioritization framework to accomplish that	**Digital Signature /Date** TREMBLAY DANIEL Digitally signed by TREMBLAY DANIEL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057 Reason: I am the author of this document Location: your signing location here Date: 2021-12-03 10:31:24 Foxit PhantomPDF Version: 10.0.1
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2021.11.29 11:36:13 -05'00'
Chief Security Officer: Pierre Lessard, Chief Security Officer and Director General, Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Digitally signed by LESSARD PIERRE Date: 2021.11.30 11:42:49 -05'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 ArriveCan V2.3 - SAVE

This application has a level of assessed risk, for which the target level of acceptable residual risk i

This Interim Security Authorization provides an interim authority to Operate with an expiry date of May 29, 2022, to process information up to and including Protected B service delivery information with availability (PBMM) commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracking Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-11-26	Y		
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracking applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2021-11-29		1.7
BSO Mobile App Lite	BSO Mobile	FSAR, SMAP	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY
BRANCH

Service Life Cycle Management
Framework (SLMF)
Baseline 3

**Security Management Control
Method (SMCM)**

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACING

VALID 2021-12-10 THRU 2022-12-10

VERSION: 1.8
DATE: 2021-12-10

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracing desktop application V1	
1.1	2020-04-16	ArriveCan Mobile Application Release 1	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	
1.7	2021-11-29	ArriveCan v2.23 – SAVE *Valid 2021-11-29 thru 2022-05-29*	2021-12-03
1.8	2021-12-	ArriveCan v2.23 – Security Uplift *Valid 2021-12-14 thru 2022-12-14*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

Signature Page

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Service Owner: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** UTANO ANTONIO Digitally signed by UTANO ANTONIO Date: 2021.12.15 14:33:45 -05'00'
CBSA Chief Technology Officer: Daniel Tremblay, Director General, IT Solutions and Operations	
Conditions:	**Digital Signature /Date** TREMBLA Y DANIEL Digitally signed by TREMBLAY DANIEL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057 Reason: I am the author of this document Location: your signing location here Date: 2021-12-13 06:22:16 Foxit PhantomPDF Version: 10.0.1
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2021.12.10 15:29:11 -05'00'
Chief Security Officer: Pierre Lessard, Chief Security Officer and Director General, Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Digitally signed by LESSARD PIERRE Date: 2021.12.10 16:25:07 -05'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 ArriveCan V2.4 – Security Uplift

This application has a level of assessed risk, for which the target level of acceptable residual risk

This Interim Security Authorization provides an interim authority to Operate with an expiry date of May 29, 2022, to process information up to and including Protected B service delivery information with availability (PBMM) commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

2.2 COVID 19 – Contact tracing desktop application V1, ArriveCan V1.0, V2.19, 2.22

The COVID 19 – Contact tracing desktop application V1 and ArriveCan Versions 1.0, 2.19 and 2.22 have been granted full Security Authorizations as the vulnerabilities detected in those release have now been mitigated and the mitigations have been reviewed and assessed. These releases now have a of assessed risk, where the target level of acceptable residual risk

This Security Authorization provides an authority to Operate to process information up to and including Protected B service delivery information with Medium Integrity and Medium availability (PBMM) commencing immediately following approval of this document.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracing Desktop Application	2020-04-03	N		N/A

ArriveCan Contact Tracing Mobile App and Backend	2021-12-10	Y		N/A
Mandatory Random Testing (MRT)	2021-10-18	Y		
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V2.24	ArriveCan Contact Tracing Mobile App and Backend	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2021-12-10		1.8
ArriveCan V2.23	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-11-29		1.7
BSO Mobile App Lite	BSO Mobile	FSAR, SMAP	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracing	FSAR, SMAP	2021-06-30		1.3

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
	Mobile App and Backend				
ArriveCan v2	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACING

VALID 2022-03-21 THRU 2023-03-21

VERSION: 1.9
DATE: 2022-03-14

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracing desktop application V1	
1.1	2020-04-16	ArriveCan Mobile Application Release 1	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	
1.7	2021-11-29	ArriveCan v2.23 – SAVE *Valid 2021-11-29 thru 2022-05-29*	2021-12-03
1.8	2021-12-10	ArriveCan v2.24 – Security Uplift *Valid 2021-12-14 thru 2022-12-14*	2021-12-15
1.9	2022-03-14	ArriveCan Backend – V3 *Valid 2022-03-21 thru 2023-03-21*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

SIGNATURE PAGE

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: John Ommanney, Director General, Travellers Policy and Programs	
Conditions:	**Digital Signature /Date** HERAGE ALYSSA Digitally signed by HERAGE ALYSSA Date: 2022.03.18 16:21:56 -04'00'
Service Owner: Kelly Belanger, Director General, Projects and Service Management	
Conditions:	**Digital Signature /Date** BELANGER KELLY Digitally signed by BELANGER KELLY Date: 2022.03.17 07:28:35 -04'00'
Cloud Competency Center: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** TSANG HIENKIEN Digitally signed by TSANG HIENKIEN Date: 2022.03.16 13:38:46 -04'00'
CBSA Chief Technology Officer: Daniel Tremblay, Director General, IT Solutions and Operations	
Conditions:	**Digital Signature /Date** TREMBLAY DANIEL Digitally signed by TREMBLAY DANIEL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057 Reason: I am the author of this document Location: your signing location here Date: 2022-03-19 21:55:53 Foxit PhantomPDF Version: 10.0.1
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2022.03.15 18:13:55 -04'00'
Chief Security Officer: Pierre Lessard, Chief Security Officer and Director General, Security and Professional Standards	
Conditions: Approving as A/DG & CSO	**Digital Signature /Date** FORTIER STEVE Digitally signed by FORTIER STEVE DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=FORTIER STEVE + SERIALNUMBER=2006026032852512 Reason: I am approving this document Location: Ottawa, Ontario Date: 2022-03-18 14:48:53 Foxit PhantomPDF Version: 10.0.1

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 ArriveCan Backend V3

This application has a level of assessed risk, for which the target level of acceptable residual risk

This Interim Security Authorization provides an interim authority to Operate with an expiry date of March 21, 2023, to process information up to and including Protected B service delivery information with availability (PBMM) commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracing Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracing Mobile App and Backend	2022-03-21	Y		
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V3 Backend	ArriveCan Backend	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2022-03-14		1.9
ArriveCan V2.24	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-12-10		1.8
ArriveCan V2.23	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-11-29		1.7
BSO Mobile App Lite	BSO Mobile	FSAR, SMAP	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3

[3] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan v2	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACING

VALID 2022-06-28 THRU 2023-06-28

VERSION: 1.10
DATE: 2022-06-28

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracing desktop application V1	
1.1	2020-04-16	ArriveCan Mobile Application Release 1	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	
1.7	2021-11-29	ArriveCan v2.23 – SAVE *Valid 2021-11-29 thru 2022-05-29*	2021-12-03
1.8	2021-12-10	ArriveCan v2.24 – Security Uplift *Valid 2021-12-14 thru 2022-12-14*	2021-12-15
1.9	2022-03-14	ArriveCan Backend – V3 *Valid 2022-03-21 thru 2023-03-21*	2023-03-19
1.10	2022-06-23	ArriveCan V3.0 *Valid 2022-06-28 thru 2023-06-28*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

SIGNATURE PAGE

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: John Ommanney, Director General, Travellers Policy and Programs	
Conditions:	**Digital Signature /Date** HERAGE ALYSSA Digitally signed by HERAGE ALYSSA Date: 2022.06.28 13:12:52 -04'00'
Service Owner: Kelly Belanger, Director General, Projects and Service Management	
Conditions:	**Digital Signature /Date** BELANGER KELLY Digitally signed by BELANGER KELLY Date: 2022.06.27 12:42:34 -04'00'
Cloud Competency Center: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** UTANO ANTONIO Digitally signed by UTANO ANTONIO Date: 2022.06.27 08:48:45 -04'00'
CBSA Chief Technology Officer: Dave Beach, a/Director General, IT Solutions and Operations	
Conditions:	**Digital Signature /Date** BEACH DAVE Digitally signed by BEACH DAVE Date: 2022.07.01 16:22:36 -04'00'
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2022.06.24 16:17:11 -04'00'
Chief Security Officer: Pierre Lessard, Chief Security Officer and Director General, Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Digitally signed by LESSARD PIERRE Date: 2022.06.29 10:40:25 -04'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 ArriveCan V3

This application has a level of assessed risk, for which the target level of acceptable residual risk

This Interim Security Authorization provides an interim authority to Operate with an expiry date of June 28, 2023, to process information up to and including Protected B service delivery information with . availability (PBMM) commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracing Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracing Mobile App and Backend	2022-06-23	Y		
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan V3	ArriveCan	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2022-06-14		1.10
ArriveCan V3 Backend	ArriveCan Backend	FSAR, SMAP	2022-03-14		1.9
ArriveCan V2.24	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-12-10		1.8
ArriveCan V2.23	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-11-29		1.7
BSO Mobile App Lite	BSO Mobile	FSAR, SMAP	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracing	FSAR, SMAP	2021-06-30		1.3

[3] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
	Mobile App and Backend				
ArriveCan v2	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY
BRANCH

Service Life Cycle Management
Framework (SLMF)
Baseline 3

**Security Management Control
Method (SMCM)**

Security Authorization (SA)

for

COVID-19 CONTACT TRACING

VERSION: 1.11
DATE: 2022-08-02

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracing desktop application V1	
1.1	2020-04-16	ArriveCan Mobile Application Release 1	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	
1.7	2021-11-29	ArriveCan v2.23 – SAVE *Valid 2021-11-29 thru 2022-05-29*	2021-12-03
1.8	2021-12-10	ArriveCan v2.24 – Security Uplift *Valid 2021-12-14 thru 2022-12-14*	2021-12-15
1.9	2022-03-14	ArriveCan Backend – V3 *Valid 2022-03-21 thru 2023-03-21*	2023-03-19
1.10	2022-06-23	ArriveCan V3.0 *Valid 2022-06-28 thru 2023-06-28*	
1.11	2022-08-02	R2094 – Mandatory Random Testing (MRT)	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

SIGNATURE PAGE

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: Mary Teresa Glynn, a/Director, COVID - 19 Border Task Force	
Conditions:	**Digital Signature /Date**
Service Owner: Carol Sabourin, Executive Director, Project and Service Management Oversight	
Conditions:	**Digital Signature /Date** SABOURIN CAROL Digitally signed by SABOURIN CAROL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=SABOURIN CAROL + SERIALNUMBER=2018194083752984 Reason: I am the author of this document Location: your signing location here Date: 2022-08-05 13:36:46 Foxit PhantomPDF Version: 10.0.1
Cloud Competency Center: Bruce Mchaffie, a/Director General, Cloud Competency Centre	
Conditions:	**Digital Signature /Date** MCHAFFIE BRUCE Digitally signed by MCHAFFIE BRUCE Date: 2022.08.02 16:48:09 -04'00'
CBSA Chief Technology Officer: Herve Madelaine, a/Executive Director, IT Operations	
Conditions:	**Digital Signature /Date**
Cyber Security: Steven Proulx, Director, Cyber Security and IT Continuity	
Conditions: acting for Steven	**Digital Signature /Date** HARGRAVE CAROLE Digitally signed by HARGRAVE CAROLE Date: 2022.08.02 11:58:55 -04'00'
Chief Security Officer: Lindsay Reeves, Director, Infrastructure and Information Security	
Conditions:	**Digital Signature /Date**

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | AUTHORIZATION PACKAGE

2.1 Mandatory Random Testing (MRT) 1.5 release (R2094)

This application has a level of assessed risk, for which the target level of acceptable residual risk i

This Security Authorization provides an authority to Operate, to process information up to and including Protected B service delivery information with availability (PBMM) commencing immediately following approval of this document. | Authorization Package – Tracking by Release

2.2 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	Last Assessment Date	Baseline Assessment Completed	Security Risk Level	Evolution of Security Posture
PHAC Contact Tracing Desktop Application	2020-04-03	N		N/A
ArriveCan Contact Tracing Mobile App and Backend	2022-06-23	Y		
Mandatory Random Testing (MRT)	2022-07-25	Y		N/A
BSO Mobile App	2021-11-25	Y		

2.3 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
R2094 MRT	MRT	FSAR	2022-07-25		1.11
ArriveCan V3	ArriveCan	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2022-06-14		1.10
ArriveCan V3 Backend	ArriveCan Backend	FSAR, SMAP	2022-03-14		1.9
ArriveCan V2.24	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-12-10		1.8
ArriveCan V2.23	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-11-29		1.7
BSO Mobile App Lite	BSO Mobile	FSAR, SMAP	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2

[3] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.

Service Name:	**COVID-19 Contract Tracing applications**				
Release[3]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
ArriveCan v1	ArriveCan Contact Tracing Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

PROTECTED A

CANADA BORDER SERVICES AGENCY
INFORMATION, SCIENCE AND TECHNOLOGY BRANCH

Service Life Cycle Management Framework (SLMF)
Baseline 3

Security Management Control Method (SMCM)

Interim Security Authorization (ISA)

for

COVID-19 CONTACT TRACKING

VALID 2021-11-26 THRU 2022-11-26

VERSION: 1.6
DATE: 2021-11-25

Revision History

This section shows the current revision of this document.

Security Authorization

Version Number[1]	Date Completed	Driver	Final sign-off completed on
1.0	2020-04-03	COVID 19 – Contact tracking desktop application *Valid 2020-04-03 thru 2020-10-03*	
1.1	2020-04-16	ArriveCan Mobile Application Release 1 *Valid 2020-04-17 thru 2020-10-17*	2020-06-16
1.2	2020-07-13	ArriveCan Release 2 *Valid 2020-07-14 thru 2021-01-14*	2020-07-14
1.3	2021-06-30	ArriveCan v2.19 – Proof of Vaccine *Valid 2021-07-05 thru 2022-07-05*	2021-07-04
1.4	2021-10-18	ArriveCan v2.22 – BSO *Valid 2021-10-18 thru 2022-10-18*	2021-11-03
1.5	2021-10-27	R1867 – Mandatory Random Testing (MRT)	2021-11-08
1.6	2021-11-25	BSO Mobile Lite *Valid 2021-11-26 thru 2022-11-26*	

[1] **Important:** Any change in the list of the Service Assets listed in section 4.1 is considered a major revision (e.g. going from 2.3 to 3.0), while any change in the security rating summary of the same section, without addition or removal of Service Assets is considered a minor revision (e.g. going from 2.3 to 2.4)

SIGNATURE PAGE

This SMCM Security Authorization (SA) has been developed and produced in accordance with ISTB's Service Life Cycle Management Framework, Baseline 3.

Approvals – Security Authorization

I have completed the review of the key evidence supporting this security authorization, including the summary of security risks in Section 2. I am granting/re-granting this information system an Interim Authorization to Operate and, in so doing, I accept the security risk to the business associated with running that system within the current operational context. The security authorization of the information system will remain in effect as long as it satisfies the requirement for continuous monitoring or that it is revoked by the authorizers.	
Program Owner: Calvin Christiansen, Director General, COVID-19 Border Task Force	
Conditions:	**Digital Signature /Date** Sharon Spicer Digitally signed by Sharon Spicer DN: CN=Sharon Spicer, E=sharon.spicer@cbsa-asfc.gc.ca Reason: I am approving this document Location: your signing location here Date: 2021-12-16 22:03:13 Foxit PhantomPDF Version: 10.0.1
Service Owner: Antonio Utano, a/Director General, Border Technologies Innovation	
Conditions:	**Digital Signature /Date** LAUZON STEVE Digitally signed by LAUZON STEVE Date: 2021.11.25 18:49:02 -05'00'
CBSA Chief Technology Officer: Daniel Tremblay, Director General, IT Solutions and Operations	
I understand and acknowledge that the Agency has determined the business benefit represented by this service significant enough to warrant the issuance of a time-limited SA pending the more comprehensive implementation of mitigations and safeguards, and I will collaborate with other stakeholders within the Agency's prioritization framework to accomplish that.	**Digital Signature /Date** TREMBLAY DANIEL Digitally signed by TREMBLAY DANIEL DN: C=ca, O=gc, OU=ccra-adrc, OU=PERSONNEL, CN=TREMBLAY DANIEL + SERIALNUMBER=2015145231123057 Reason: I am the author of this document Location: your signing location here Date: 2021-12-03 06:58:44 Foxit PhantomPDF Version: 10.0.1
Cyber Security: Gino Lechasseur, Director General, Enterprise Collaboration and Digital Services	
Conditions:	**Digital Signature /Date** LECHASSEUR GINO Signature numérique de LECHASSEUR GINO Date : 2021.11.25 17:07:06 -05'00'
Chief Security Officer: Pierre Lessard, CSO and Director General, Security and Professional Standards	
Conditions:	**Digital Signature /Date** LESSARD PIERRE Digitally signed by LESSARD PIERRE Date: 2021.11.26 09:20:27 -05'00'

Section 1 | Security Authorization (SA) Content

The Security Authorization (SA) document conveys the final security authorization decision from the authorizing officials to grant an "Authorization to Operate - ATO" and, in so doing, accepts the risk to the business associated with running that system within the current operational context.

The explicit acceptance of risk is the responsibility of the authorizing officials and cannot be delegated to other officials within the organization. For all SA, the authorizing officials include, as a minimum:

I. The IT-Enabled Service Business Owner
II. The IT-Enabled Service Owner
III. The Departmental Security Officer

The authorizer may issue an ATO, with or without conditions, or issue a denial of Authorization to Operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

Authorization is a state that an information system is in during the operations and maintenance phase of its lifecycle. It is not a condition that expires after a period of time and that needs to be renewed. The SA is an ongoing process. Once in operation, an information system is subjected to continuous security monitoring and assessment by the responsible IT security group.

The terms and conditions for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider.

1.1 Security Authorization in the context of SLMF

The SLMF has established the concept of "IT-Enabled Services" as the unit of management of service assets such as software applications. The decision to grant a SA is also performed at the IT-Enabled Service level.

The security posture a service is the sum of the security risks of its primary assets.

Important: The SA does not pertain to a "Solution", which typically integrates multiple IT-Enabled Services. Each Service must have its own SA. The security posture of a "Solution" is the sum of the security posture for all the services that are integrated by the solution. Acceptance of the security posture of a "Solution" is a Programs function, which is not in scope of the present SA.

Although a release typically pertains to assets of a single service, a release may also impact the security posture of multiple services. In these situations, that release may require more than one SA. By the same token, a release may pertain to a single service but affect multiple primary assets, in this case it would only require a unique SA.

Section 2 | Authorization Package

2.1 BSO Mobile Lite

This application has a [redacted] level of assessed risk, for which the target level of acceptable residual risk [redacted]

This Interim Security Authorization provides an interim authority to Operate with an expiry date of November 26, 2022, to process information up to and including Unclassified service delivery information with [redacted] ıvailability commencing immediately following approval of this document.

1. The actions identified in the Security Management Action Plan (SMAP) document are addressed following the timelines identified within the SMAP, and evidence of their implementation is provided to Cyber Security's Risk Assessment and Consultation team for re-assessment.

Section 3 | Authorization Package – Tracking by Release

3.1 Authorization Package – Summary of Security Risks

The Authorization Package is the sum of the work products supporting the Security Authorization. This will normally include all the SLMF work products pertaining to the Primary Assets of the IT-Enabled Service.

The assessment of security controls for each Service Assets is completed as a distinct work product, either as part of a Service Release or a Service Baseline Security Assessments.

The details of the determination of the Security Risks Level are subject to a distinct Security Assessment Report. Only a summary is presented here.

Asset	**Last Assessment Date**	**Baseline Assessment Completed**	**Security Risk Level**	**Evolution of Security Posture**
PHAC Contact Tracking Desktop Application	2020-04-03	N	[redacted]	N/A
ArriveCan Contact Tracking Mobile App and Backend	2021-06-30	Y		Improved
Mandatory Random Testing (MRT)	2021-10-18	Y		N/A
BSO Mobile App	2021-11-25	Y		

3.2 Authorization Package – Tracking by Releases

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SMC Review.

Each Service Assets impacting the security posture of a Service is normally security-assessed as part of a Release. The table below provides information as to which version of the SA is associated with a specific Release, where it will support the ORR SEMC Review.

Service Name:	**COVID-19 Contract Tracking applications**				
Release[2]	**Service Asset(s) impacted**	**Type of security work product completed product**	**Date**	**Security Impacts**	**Resulting version of SA**
BSO Mobile App Lite	BSO Mobile	Final Security Assessment Report (FSAR) Security Management Action Plan (SMAP)	2021-11-25		1.6
R1867 MRT	MRT	FSAR	2021-10-18		1.5
ArriveCan V2.22	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-10-18		1.4
ArriveCan V2.19 PVC	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2021-06-30		1.3
ArriveCan v2	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-07-13		1.2
ArriveCan v1	ArriveCan Contact Tracking Mobile App and Backend	FSAR, SMAP	2020-04-16		1.1
PHAC Desktop	Interim Security Authorization	Interim Security Authorization (ISA)	2020-04-03		1.0

[2] **Important:** Unless otherwise specified, Maintenance Releases (MR) are **not** included in the tracking. Maintenance Releases have, by definition, low security impact and are reviewed through a separate process. Where a MR is considered to have a potential impact on the security posture of a Service, it may be included here, as an exception, and be subject to a Security Authorization.